



nonce "mutual authentication"

1996

1999

Search

Ad
Sci
Sci

Scholar

Results 1 - 10 of about 86 for nonce "mutual authentication". (0.09 seconds)

Mechanized proofs for a recursive authentication protocol - group of 13 »

LC Paulson - PROC COMPUT SECUR FOUND WORKSHOP, 1997 - doi.ieeecomputersociety.org
 ... protocol delivers session keys for all the agents, allowing neighbours to perform
mutual authentication. ... round, an agent adds its name and a fresh **nonce** to an ...
Cited by 79 - Web Search - Library Search

An Authentication Protocol Without Trusted Third Party - group of 3 »

SP Shieh, WH Yang, HM Sun - IEEE COMMUNICATIONS LETTERS, 1997 - ieeexplore.ieee.org
 ... (herein can be considered as a **nonce** of user ... Tanaka's scheme, each party needs five
 exponential computations to complete **mutual authentication** and exchange ...
Cited by 16 - Web Search - BL Direct

A survey of authentication protocol literature: Version 1.0 - group of 14 »

J Clark, J Jacob - University of York, Department of Computer Science, November, 1997 - win.tue.nl
 ... 64.6.10.2 Gong **Mutual Authentication Protocol** ... We shall sometimes refine the notion
 of a **nonce** to include a timestamp and distinguish between sequence numbers ...
Cited by 109 - View as HTML - Web Search

Security protocol for IEEE 802.11 wireless local area network - group of 10 »

SH Park, A Ganz, Z Ganz - Mobile Networks and Applications, 1998 - Springer
 ... also has a unique merit as compared with other approaches which use **mutual**
authentication proto- cols or hand-shake methods, because we never expose the **nonce**. ...
Cited by 17 - Web Search - BL Direct

Mutual Authentication with Smart Cards - group of 3 »

B Bakker - USENIX Workshop on Smartcard Technology, may, 1999 - usenix.org
 ... ABK(t) type protocol, named KLOMP (KryptoKnight-based Lightweight Open **Mutual**
authentication Protocol ... is possible because the search for a suitable **nonce** can be ...
Cited by 4 - Web Search

Some new attacks upon security protocols - group of 15 »

G Lowe - PROC COMPUT SECUR FOUND WORKSHOP, 1996 - doi.ieeecs.org
 ... they who initiated the protocol run; or (2) the agents may disagree over the value
 of some **nonce** exchanged dur ... 3. The Woo and Lam **mutual authentication** protocol ...
Cited by 90 - Web Search

[ps] Using non interference for the analysis of security protocols - group of 7 »

R Focardi, A Ghelli, R Gorrieri - Proceedings of DIMACS Workshop on Design and Formal ..., 1997 -
 lix.polytechnique.fr
 ... The aim of the Needham-Schroeder protocol [NS78] is to establish **mutual authentication**
 between two users A and B. It uses public key cryptography. ...
Cited by 55 - View as HTML - Web Search

[ps] Towards extensional goals in authentication protocols - group of 2 »

C Boyd - Proceedings of the 1997 DIMACS Workshop on Design and Formal ..., 1997 - dimacs.rutgers.edu
 ... a **nonce** is associated with a specific party, or whether a **nonce** was received ... They define
 a se- cure **mutual authentication** protocol as one in which two principals ...
Cited by 22 - View as HTML - Web Search

An efficient authentication protocol for mobile networks - group of 6 »

SP Shieh, FS Ho, YL Huang - Journal of Information Science and Engineering, 1999 - iis.sinica.edu.tw

... session key successfully and verified the freshness of the **nonce**, the identity ...authentication proto- col can also be eliminated if **mutual authentication** is not ...Cited by 7 - View as HTML - Web SearchScalability and Flexibility in Authentication Services: The KryptoKnight Approach - group of 10

»

P Janson, G Tsudik, M Yung - IEEE INFOCOM, 1997 - doi.ieeecomputersociety.org

... and B stand for the identifiers of two network entities performing **mutual****authentication**. ... number of message flows (three) is minimal for a **nonce**- based protocol ...Cited by 20 - Web Search - BL Direct

Gooooooooogle ►

Result Page: 1 2 3 4 5 6 7 8 9 Next [Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2006 Google